webMethods API Gateway 10.5 Readme

October 2019

This file contains important information you must read before using webMethods API Gateway 10.5. You can find system requirements, user documentation, and installation and upgrade instructions on the Documentation website or the TECHcommunity website. At those locations, you can also find suite-related security and globalization information.

Included in this file is information about functionality that has been added, removed, deprecated, or changed for this product. Deprecated functionality continues to work and is supported by Software AG, but may be removed in a future release. Software AG recommends against using deprecated functionality in new projects.

1.0 Critical Information

This section lists any critical issues for the current release that were known when this readme was published. For critical information found later, go to the Knowledge Center on the Empower website.

2.0 Known Issues

This section lists any issues for the current release that were known when this readme was published. For known issues found later, go to the Knowledge Center on the Empower website.

- YAI-7189
  API associated with a package is allowed to be deleted.
  An API, which is associated with a package, is deleted and imported again using export archive of the API, the association of API and Package is created automatically.
- PIE-53165
  Registration port cannot be updated.
  API Gateway port update returns with an empty message box. In addition, the ports are removed and not visible in the API Gateway user interface.
- YAI-13095

  Passman data is not migrated to 10.5
  Migration of older versions of API Gateway to 10.5 version of API Gateway is incomplete if passman data is part of migration.
- YAI-13084

  Backup of data is not processed

  Data backup command is not adhered. However, to workaround this issue and get the backup, create the index "gateway_default_dummypolicyaction" in Elasticsearch.
- YAI-12255

  Primary port is deleted with REST call.

  Port marked as primary should not be allowed to be deleted. The primary port is not allowed to be deleted form UI. However, the primary port can be deleted using a REST API call.

3.0 Usage Notes

This section provides any additional information you need to work with the current release of this product.

- Before using API Gateway, consider the following points:
  - API Gateway package in Integration Server cannot co-exist with the WmMediator or WmCloudStreams packages. WmMediator and WmCloudStreams packages must be disabled

for API Gateway to function properly.

- webMethods API Gateway combines current webMethods Enterprise Gateway and webMethods Mediator capabilities in a single product. API Gateway offers the same capabilities within a simplified architecture. It also removes the dependency on CentraSite for API definition and policy definition.

- API Gateway comes in two editions. The Standard edition allows users to define threat protection policies, and provides analytics for threat protection use cases. Typically Standard editions are deployed in DMZ.
  Full edition supports all use cases of Standard edition, supports managing APIs, consumer applications, API-level policies, and managing API packages and plans.

- When API Gateway and API Gateway Data Store are already running and IP address is changed, connection between API Gateway and the Data Store is lost. Restart the API Gateway Data Store to reconnect to API Gateway.

- API Gateway uses the `pub.client:http` IS service to invoke HTTP based services.

  - An Integration Server property 'watt.net.http401.throwException' allows the `pub.client:http` service to throw NetException for a 401 Unauthorized response from native service. This property was by default set to 'true' in Integration Server (in the Integration Server Administrator, go to Settings > Extended link). As a result, the response from API Gateway did not include the native service response body in case of 401 responses from native service. Beginning with API Gateway version 10.3, the watt.net.http401.throwException property is by default set to ‘false’ in Integration Server. Now, the `pub.client:http` service will not throw a NetException for 401 unauthorized responses from the native service. API Gateway will receive the 401 response body and send the native API provider's fault content (if available) to the application if the Send native provider fault option is enabled in API Gateway (in the API Gateway user interface, go to Username > Administration > General > API fault).

  - An Integration Server property 'watt.net.http501-599.throwException' allows the `pub.client:http` service to throw NetException for a HTTP response status code that varies from 501 to 599 from native service. This property was by default set to 'true' in Integration Server (in the Integration Server Administrator, go to Settings > Extended link). As a result, the response from API Gateway did not include the native service response body in case of 501 to 599 responses from native service. Beginning with API Gateway version 10.3, the 'watt.net.http501-599.throwException' property is by default set to ‘false’ in Integration Server. Now, the `pub.client:http` service will not throw a NetException for HTTP 501 to 599 responses from the native service. API Gateway will receive the 501 to 599 response body and send the native API provider's fault content (if available) to the application if the Send native provider fault option is enabled in API Gateway (in the API Gateway user interface, go to Username > Administration > General > API fault).

Note: These configuration changes may negatively impact any webMethods product instance which is installed with an instance of Integration Server on which API Gateway is running. Software AG

recommends that you use an instance of Integration Server dedicated for API Gateway.

4.0 Fixes Included in Each Release

This section lists the latest fix level that has been included in each release for each product component. A release is listed in this section only if changes occurred in that release. Go to the Knowledge Center on the Empower website for detailed information about fixes.

Release 10.4

- YAI_10.4_Fix3

Release 10.3

- YAI_10.3_Fix10

Release 10.2

- YAI_10.2_Fix5

Release 10.1

- YAI_10.1_Fix20

Release 10.0

- YAI_10.0_Fix9

Release 9.12

- YAI_9.12_Fix9

5.0 Other Resolved Issues

This section lists the issues that were resolved in each release but were not part of the fixes listed in the previous section. A release is listed in this section only if changes occurred in that release.

6.0 Documentation Changes

This section describes significant changes to the documentation, such as the addition, relocation, or removal of product guides, online help, chapters, or other major content. A release is listed in this section only if changes occurred in that release.

Release 10.3

The following artifacts have been introduced for API Gateway 10.3:

- webMethods API Gateway WebHelp: This is single HTML output that contains all the PDFs available for API Gateway on Empower.

Release 10.0

The following artifacts have been introduced for API Gateway 10.0:

- webMethods API Gateway Quick Start Guide: This is single page PDF output that gives an overview of setting up API Gateway.

Release 9.12

The following artifacts have been introduced for API Gateway 9.12:

- webMethods API Gateway Online Help
- webMethods API Gateway User's Guide: This guide describes how you can use API Gateway and other API Gateway components to effectively manage APIs for services that you want to expose to consumers, whether inside your organization or outside to partners and third parties.
- webMethods API Gateway Configuration Guide: This guide describes how you can configure API Gateway and other API Gateway components to effectively manage APIs for services that you want to expose to consumers, whether inside your organization or outside to partners and third parties.

7.0 Terminology Changes

A release is listed in this section only if changes occurred in that release.

8.0 Added, Removed, Deprecated, or Changed Items

This section lists features, functionality, controls, portlets, properties, or other items that have been added, removed, deprecated, or changed. A release is listed in this section only if changes occurred in that release.

Release 10.5

Added Item	Description
Custom Runtime Policies	API Providers can now invoke any external services, which can act as a runtime policy as part of the policy enforcement and thus can support custom runtime policies. Custom policies can be included in the stages such as, Identify and Access or Payload processing stages, or Routing stage. AWS Lambda functions also can be considered for custom policies.
Team work Support	Team work support is to provide access control based on team-specific privileges in the deployments where multiple teams work on a single API Gateway instance. Assets of type API, Application, Package, Plan would be team-specific in such deployments and deployments where teams is not applicable, this can be switched off.
API First	API-first is an approach where the design and development of an API comes before the implementation. API Gateway can now cater provider-complaint specification that can be used to register API first in API Gateway as part of API-first approach.
Externalization of configurations	Inter-component configurations and cluster configurations are available at different locations causing maintainability and operational overhead. A new centralized configuration management is introduced in this version where configuration of API Gateway, Kibana, and filebeat connections to Elasticsearch and API Gateway, Elasticsearch and Terracotta cluster configurations for clustering is supported.
Command Central integration	API Gateway integration with Command Central is enhanced for managing API Gateway instances through Command Central for Logs, Ports, Licensing, and Clustering configuration. The same is supported now through Command Central templates as well.

Added Item	Description
Change ownership of Assets	Ownership of API and Application type assets can be transferred to a different user and can be implemented with Approval flow if desired. This would help to overcome the unavailability of specific data in the case where the current owner is not available in the system.
Governed API development	APIs provided by CentraSite are considered read-only if a CentraSite destination is configured. If there is no CentraSite destination there is no connection to CentraSite and therefore no read-only restriction needs to be enforced. Scopes and policies can still be updated in API Gateway.

Changed Item	Description
Internal Data Store	Internal Data Store is now renamed to API Gateway Data Store. API Gateway 10.5 is updated to use Elasticsearch 7.2.0 only as its data store.
Access Profiles	Access profiles are now changed to Teams

Release 10.4

Added Item	Description
Import and Export Enhancements	Import and export support that was limited to some assets is now enhanced to include all assets and configurations so that users can easily move the configurations across instances.
Staging and Promotion Enhancements	Staging and promotion support that was limited to some assets is now enhanced to include all assets and configurations so that users can easily move the configurations across instances. Aliases can be configured with stage details.
Support Certificates in Custom Headers	Application identification is enhanced to get certificates sent through Custom HTTP header in order to identify the application. Custom header can be configured as part of extended settings of Administration.

Added Item	Description
Support API Composition in API Mashups	API providers can configure to invoke multiple APIs as part of mashup step and aggregate the response that is passed to the next step. Similarly responses of different steps can be aggregated and sent as single output to the client.
Microgateway Management in API Gateway	API Gateway displays list of live Microgateways registered to it and are now able to retrieve details about list of assets, and configurations of each Microgateway.

Changed Item	Description
Application Identification	In case of Application identification failure, error message is changed from Unable to identify the application for the request to Unauthorized application request.

Release 10.3

Added Item	Description
Open API Support	Users can create an API by importing an open API document file or URL in API Gateway. OpenAPI Specification (formerly Swagger Specification) is an API description format for REST APIs.
Support for API Mashups	Individual microservices and APIs can be composed into one mashed up API. API Gateway handles a request by invoking multiple microservices and aggregating the results and provide final response.
Support Async APIs	APIs which take longer than usual invocation time, may end up with Read Time out. API Gateway could enforce policies to use the callback URL defined for the APIs.
Support AMQP protocol	Support AMQP as an inbound and outbound endpoint for API Gateway APIs of type SOAP and REST. AMQP is open standard for passing messages between applications and provides standard messaging protocol across platforms.

Added Item	Description
API hot deploy	API updates can be done without deactivating or affecting the ongoing requests. Each request finishes without being affected by updates to the API and policy definition.
Support runtime service registries	API Gateway APIs can be published to service registries and clients can get the endpoints from service registry. APIs routing endpoint can be configured with service registry to discover endpoint from registry during outbound.
Log aggregation	API Gateway aggregates different log files used for logging API Gateway usage and provides a comprehensive log file. Logs can be also viewed in the dashboard with filtering capabilities.
Security enhancements	Security configuration is unified for OAuth, OpenID and JWT configuration, and is simplified. Support for multiple active Authorization servers simultaneously is included. Added capability to register clients dynamically in third-party Authorization servers. Support for third-party clients introspection. PKCE client application support for third-party Authorization servers. Mapping of OAuth scopes with API scopes.

Removed Item	Replacement, if any
Inbound Authentication – Transport policy was removed from API Gateway10.3	This functionality was added into the Identify and Authorize Application policy.

Release 10.2

Added Item	Description

Added Item	Description
API Tagging	APIs or its resources and operations can be tagged. You can use the tags for searching artifacts in API Gateway and publish the tags along with the API to API Portal. API creation using Swagger can acquire the tags from the swagger file and also API export should include the assigned tags.
Bulk Publish, Unpublish and Delete	You can publish, unpublish or delete more than one API at a time to API Portal.
File attachments support for API	APIs can be attached with supporting files as attachments and the attached files are available in API Portal after publishing to the Portal.
JWKS endpoint for JSON Web Tokens	As an ID provider, API Gateway provides the JWKS endpoint that helps the relying parties to fetch the certificates that can be used for validation of the JSON Web tokens.
HTTP Client for Elastic Search	Relaxes the hard limitation of using the Elastic search shipped along with API Gateway product; you can use other elastic search instance configured with API Gateway
Application suspension	You can now suspend applications to deactivate the runtime access to the applications in API Gateway and the same application can be activated again.
CORS Support in API gateway	API Gateway can process cross origin requests sent by clients as inbound policy and also as transparent mode of native service processing cross origin requests.
Specification for Invoke IS Service	You can now define IS Service to get and set headers, status code, body, and other MessageContext variables using the specification in the service and do not have to write code to extract the variables.
Enhance Transaction events	Transaction events are enhanced to log headers and query parameters of request and response along with the payload.

Added Item	Description
Caching enhancements	You can manage different caches of API Gateway to auto scale or allocate static percentage of data to be held in cache.
Data masking	API Gateway's data masking policy can be configured to mask or filter specific data in request and response messages and also mask the data in transaction events.
JSON Schema and JSON Path Support	JSON payload can be evaluated for schema validation and JSON path can be used in policies like content-based routing, error processing, and identify application.
User profile management	You can now configure your preferences like name, email passwords, and display language.
Audit logging support	Audit logging would capture user activities in API Gateway for API, application, approvals, and user management. Audit logs would capture who has done the action and when. These logs help in securing the system.
API Monetization	Plans and packages can be managed by quotas, usage, and rate limits with soft and hard limits. Consumers can subscribe to plans and monitor usage and re-subscribe as required.

Release 10.1

Added Item	Description

Added Item	Description
Migration from Mediator to API Gateway	APIs and associated data can be published from CentraSite to API Gateway 10.1 version. This allows users to publish Virtual Services of SOAP and REST with applied policies, consumer applications, runtime alias to API Gateway, which play the role of policy enforcement point and replace Mediator.
Migration from Enterprise Gateway to API Gateway	Enterprise Gateway configurations and Rules can be migrated to API Gateway, which replace and play the role of Enterprise Gateway.
Staging and Promotion support	You can now promote assets from one stage to another. API Gateway uses webMethods Deployer for promoting assets across stages. Promoting an asset involves calculating its dependencies and promoting them unless explicitly specified by the user. Stage-specific configurations and alias values can be modified to respective values. API Gateway assets can be managed with version control system and perform scheduled or automatic promotion to stages as configured.
Support for SOAP over JMS	Support JMS protocol of Inbound and Outbound for SOAP. Allow JMS-HHTP bridging between Inbound and Outbound.
Backup and Restore	Backup API Gateway assets and configuration using command line and you can restore the backed up data.
Transaction based licensing	License model based on transactions and appropriate alerts can be implemented
Approval model for applications	Approval model can be implemented for creating or updating applications, associating applications with APIs, and subscribing to packages.
API Mocking	Mocking mode allows users to make mock calls to APIs. User can specify API response for each resource or operation and can set status codes for responses. API responses can be configured on conditional basis too.

Added Item	Description
Support 3rd party OAuth providers	Users can use 3rd party Authorization Servers for authenticating API invocations using OAuth2 Third party OAuth2 providers like OKTA and Ping Federate can be used for OAuth2 authentication.
Support JSON Web Tokens	API Gateway can authenticate clients using JSON Web Tokens supplied during invocations.
Open ID Support	API Gateway can authenticate clients using Open ID Tokens supplied during invocations.
HTTP Header Validation	Providers can mandate consumers to send HTTP headers and values defined in policy for API Invocations.

Release 10.0

Added Item	Description
API Versioning	New version for an API can be created. Different versions of an API can be viewed and invoked
SOAP to REST transformation	API Provider can enable some of the operations of SOAP service as REST endpoints. These operations can be invoked with different paths and the operation path can contain Path parameters that can be saved as templates and can be hierarchical. The operation can be invoked in a method other than POST
API export and import	APIs in API Gateway can be exported and imported into a different API Gateway. This implies that the export archive for an API includes all the information to establish an API in the importing API Gateway.
Support Service Result Cache	Service result of the first invocation is cached when the criteria defined in the policy is met. Subsequent requests are from cache and do not require to go to native service for every similar invocation.

Added Item	Description
Schema Validation Support	Validates the incoming requests and responses against a schema referenced in the WSDL for SOAP APIs. For REST API, user should be able to validate incoming requests and responses against the specified schema.
API usage reports and dashboards	Package-level and API-specific usage and utilization reports. API Gateway provides number widgets for package invocations and API invocations.
Archive purge and restore events data	Administrators can archive and purge events data to a configured file location. The archived data is restored from the created archives.
Resources or Operation level policies	Policies can be applied to one or more resources or operations and must be applied on an API always. Scope can be created with a collection of resources, methods or operations of an API and policies can be applied to the scope to apply to the specific operation or resources.
Global policies and policy templates	Global Policy is a common policy that can be associated to multiple APIs based upon the criteria defined for the policy. Policy Template is a base template defined, which can be imported in multiple APIs.
SAML Authentication	APIs can be applied with SAML authentication policies at Inbound and Outbound. Bearer and Holder of Key SAML subject confirmation are supported for SAML 1.0 and 2.0 versions.
Kerberos Authentication	Kerberos authentication is supported at message and transport level for SOAP APIs and at transport level for REST APIs. APIs can be applied with Kerberos authentication policies at Inbound and Outbound.
XML Threat Protection Support	API Gateway application should be resilient to attacks through XML payload. XML payloads sent through external port go through the XML threat protection filter when the rule is defined and enabled.

Added Item	Description
JSON Threat Protection Support	API Gateway application should be resilient to attacks through JSON payload. JSON payloads sent through external port go through the JSON threat protection filter when the rule is defined and enabled.

Release 9.12

Added Item	Description
API CRUD	Both REST and SOAP APIs can be imported. Swagger and RAML are supported formats for REST and WSDL for SOAP. REST APIs can be created from scratch as well.
Policies and Aliases CRUD	Both threat protection and API-specific policies based in selected edition. For more information, see documentation for supported policies. Create and manage aliases that improve the reuse and maintenance.
Consumer Applications CRUD	Manage consumer applications and associations with APIs.
Packages and Plans	Organizations can group APIs and define enforcements on the same as a single unit, which can be subscribed by developers.
API Portal Integration	APIs can be published to API Portal from API Gateway for the developers reach.
Analytics	API Gateway provides dashboards for greater insights on various topics like Summary, Trends, Consumer applications, and Threat protection.

9.0 Copyright Information

10.0 Support

Visit the Empower website to learn about support policies and critical alerts, read technical articles and papers, download products and fixes, submit feature/enhancement requests, and more.

Visit the TECHcommunity website to access additional articles, demos, and tutorials, technical information, samples, useful resources, online discussion forums, and more.

YAI-RM-105-20191015